# The Essential Guide to Network as a Service (NaaS)

SITUATION PUBLISHING | CISCO

## Executive Summary

It is early days yet for Network as a Service. But it is already clear that NaaS will enable enterprises and other organizations to operate their network infrastructure with superior cloud-like manageability, agility, flexibility, and resilience. This will have pervasive implications across corporate infrastructure, allowing organizations to move at the pace of the business as they deploy new workloads and applications without being constrained by traditional, rigid networking approaches.

For networking specialists, the automation and optimization that NaaS promises means that they will be freed up to take on more challenging and high-value work, whether that is enabling true hybrid multi-cloud, better aligning infrastructure with business requirements, or enabling innovative new applications and workloads that support the business strategy.

Likewise, security specialists will benefit from better visibility across the network, enhanced integration, automated patching and updating, and faster remediation.

The organization as a whole will benefit from the ability to use more public network connectivity, and to exploit cloud services from any endpoint, with end-to-end security.

But to benefit from all of this, organizations must ensure they approach NaaS in the correct way from the start. Infrastructure leaders should come together with their counterparts across the organization, including HR and finance, to establish the outcomes they all desire.

NaaS reduces the total cost of connectivity and security for customers and frees organizations from the rigidity of traditional, multi-year refresh cycles, and it also represents a more open-ended, long-term journey. So, it is crucial from the outset that companies choose partners that provide both the breadth of technology and in-depth knowledge that can fully deliver this new way of networking.

## 1. Introduction

This paper presents a guide to Network as a Service (NaaS). We will share the essential fundamentals that will help you prepare your organization for NaaS. And we will give you some important guidelines on what to look for in both a NaaS offering and NaaS supplier. Most importantly, we will explain how NaaS can help you turn the network from a passive platform into a springboard for innovation and digital transformation, not least by making it easier for users to exploit SaaS applications, securely, wherever they happen to be.

### Cloud paved the way

Over the last decade the cloud has profoundly changed how organizations deploy and consume software, compute and storage. This has delivered increased agility and resilience and helped pave the way for digital transformation.

It has also changed the financial equation around enterprise computing and by enabling automation of previously manual processes, freed up highly skilled staff to tackle new challenges, increase efficiency, and deliver innovation.

But all of this has left the network largely untouched. Networks and networking infrastructure have traditionally been designed with stability and consistency in mind. This has typically meant large, upfront capital investments and time horizons of three to five years or even longer. It has also left organizations managing expensive MPLS infrastructure and tied into inflexible connectivity agreements typically involving leased lines. Yet a new trend is emerging as customers are evolving away from private MPLS in favor of Wide Area Network (WAN) of choice Internet as a suitable alternative.

Networking teams have increasingly been left out of sync as the rest of the organization evolved. Developers and lines-of-business teams have come to expect increased control, even self-service deployment, of technology resources.

### Complexity and security challenges

Meanwhile, network teams must deal with the increasing complexity due to the growing number of users, devices, expansion to cloud, distributed apps, and more of those applications running outside the corporate network. This additional complexity leaves network teams with their hands full just trying to keep the lights on.

At the same time, as the Internet becomes the WAN of choice for many customers, traffic and data has shifted outside of the traditional enterprise perimeter, with organizations managing increasingly dispersed workforces and using more disparate cloud platforms and apps, and new edge applications. These trends have become even more pronounced over the course of the COVID-19 pandemic.

Security too is no longer an issue of defining and patrolling a fixed enterprise perimeter, and IT teams need greater visibility even beyond the corporate network, and into the cloud. Security threats have become more pervasive and sophisticated, with ransomware, malware and phishing capable of crippling not just companies but entire swathes of national infrastructure.

These are the challenges that Network as a Service is designed to solve. NaaS is a flexible networking model that creates a consolidated operational and consumption solution, combining client connectivity, network service, observability, security capabilities support, and adoption services in one platform.

## 2. NaaS - What and Why

### 2i) NaaS - a working definition

> "This opens the path for users to optimize their entire infrastructure"

As a nascent consumption model, understandably the industry is still defining NaaS.

**Cisco's definition for NaaS.** Cisco's definition for NaaS is *"a cloud model that enables users to easily operate the network and achieve the outcomes they expect from it without owning, building, or maintaining their own infrastructure."* In essence, an organization is consuming networking services as a solution, transacted as a perpetual subscription or utility. This model transfers responsibility of design, integration, configuration, performance, capacity and lifecycle management to a NaaS solution provider.

> According to IDC, Enterprise NaaS can be understood as "enterprise network infrastructure that is consumed via a flexible consumption operating expense (opex) model, inclusive of: hardware, software, management tools, licenses and lifecycle services."

It's important to understand that NaaS can, and should, encompass more than just pure networking functionality. As illustrated by the shift to Secure Access Service Edge (SASE) solutions, networking and security are increasingly integrated and, as such, it's an essential part of the NaaS offering, not least because there is no perimeter – in the traditional sense – to protect.

Extending these descriptions, NaaS allows you to replace your organization's ownership and lifecycle management responsibility for network elements such as VPNs, firewalls, WAN routers and connections, and wired and wireless LANs. The core network command and control moves to the cloud, where it can be managed and monitored centrally.

As well as eliminating the upfront costs of traditional hardware and making the ongoing cost of managing and maintaining the network more transparent, this opens the path for users to optimize their entire infrastructure for key users, devices, applications, or workloads, and deploy services rapidly and scale their infrastructure up and down as business demand changes.

**Lifecycle management and proactive support.** The centralized network lifecycle management is a key component that NaaS enables, and it will be supported by advanced telemetry and predictive analytics.

It will also support new levels of observability and proactive support, meaning teams are not just informed there is a problem but are provided with actionable insights to help them isolate and fix it. These can all be harnessed to support service-level agreements (SLAs) and service-level objectives (SLOs) which are focused on the customer's desired outcomes.

## 2ii) Why NaaS?

In today's market landscape, many organizations have changed their technology consumption and execution strategies, moving towards more SaaS and IaaS services, and allowing their users secure access to any resource from anywhere. This presents complexity in network and security implementation, operation, and adoption, and creates security vulnerabilities and operational overhead for organizations.

**Flexibility and performance.** The traditional approach to infrastructure emphasized stability at the cost of flexibility. This was desirable, or at least tolerable, when enterprises could be assured that most data was created, moved and consumed within their own perimeter. However, several trends are pushing the network to be more flexible while maintaining performance and reliability.

**Data moving beyond the data center.** With the rise of the cloud, users, applications, traffic, and data has increasingly moved outside of the traditional bounds of the enterprise. By 2022, 50 percent of mission-critical apps will be hosted in public clouds, according to Gartner. Workers rely on cloud-based productivity applications to do their work, and cloud-based platforms to collaborate with their colleagues. New 5G and IoT-enabled applications require ultra-low latency and highly distributed compute and storage infrastructure supported by networking services.

**Distributed workforces.** These trends have been exacerbated by the increasing dispersal of workforces – and endpoints – which has been turbocharged by the pandemic. In a recent survey, "58 percent of office workers anticipate that they will work eight or more days each month from home." With remote or hybrid workforces set to be the norm in the future, it will be unacceptable for organizations to deliver a second-class experience to employees who are working from home or in other off-site locations.

**Distributed applications.** Modern enterprise applications are becoming highly distributed, predicated on containers and microservices, while the methodologies underlying them, such as DevOps and Continuous Delivery, presuppose that developers have access to self-service infrastructure deployment. Likewise, AI and Machine Learning, and the Internet of Things are changing the dynamics of data, whether in creating vast streams of machine data or pushing processing to the edge.

This creates challenges for management, visibility, security, and ensuring consistent quality of service wherever workers and devices are located. The changing nature of enterprise workloads and applications creates additional pressures on legacy approaches to deploying and managing network infrastructure.

**Accessing new technologies.** Networking technology itself is evolving rapidly, with new underlying technologies such as Wi-Fi 6 and 5G, and new architectural models such as SD-WAN and SASE (secure access service edge). Rigid plans based on three- or five-year cycles run the risk of leaving companies unable to access or exploit new technologies.

Network complexity is further fueled by the inevitable consolidation and splitting of networks as organizations and companies evolve, merge, divest and expand their operations.

**Staffing challenges.** The technological arms race also leads to a scramble for skilled staff – only for those highly skilled individuals to spend an increasing amount of time managing and maintaining infrastructure, not least because of rigid, inefficient legacy approaches to managing complex networks. This holds them back from grappling with how to match the network to the broader aims of the organization, now and into the future.

And all the time, networking specialists see their colleagues in the rest of the organization benefit from the shift to the cloud, or to cloud-like infrastructure, with greater ease of management, flexibility and scalability, and ask themselves, why can't this apply to networking infrastructure? And for many organizations a NaaS offering is the answer.

## 3. Simplicity and flexibility: What a NaaS solution should look like

> "Take advantage of new technology and services as they are continuously released, rather than await a new refresh lifecycle"

**Hardware included.** There have been subscription-based offerings covering networking software components for some time. However, this model has not encompassed the underlying hardware infrastructure.

A true NaaS offering would also include hardware, and associated services, along with the required software, and management capabilities, all supplied under a single subscription.

**Flexible consumption.** The subscription should include the ability to be billed for what is used. This capability provides customers better visibility into their actual consumption, and the ability to expand or scale up services as needed. For example, a retailer might plan to add sites and need to scale up connectivity – and reduce latency for payments providers – during particularly busy shopping periods.

**Predictable costs.** As well as giving customers better insight into the day-to-day cost of their networking and associated services, this subscription model gives them far more predictability when they contemplate future networking costs.

**NaaS vendor or provider owns the hardware and software.** A NaaS offering will necessarily include some customer on-premises equipment, but ownership of this – and the accompanying responsibilities for managing and maintaining it throughout its lifecycle – would remain with the NaaS service provider. As technology changes, customers will not be bound by a capital investment strategy decided three or five years previously.

NaaS will not necessarily cover underlying connectivity infrastructure – leased lines, public internet infrastructure – although this could be supplied as part of a NaaS package from a managed service provider or telco.

**Managing NaaS from the cloud.** Beyond the underlying hardware, the core networking management functionality moves to the cloud. A NaaS offering will include a central management hub and dashboard, in the cloud, that allows customers and partners to set and enforce policies, manage the services and products they need to scale them up or down, as well as suspend and eventually retire them. This should include the ability to quickly take advantage of new technology and services as they are continuously released, rather than await a new refresh lifecycle.

**Updates and security.** A basic aspect of a NaaS offering should cover the Lifecycle Management of updates, including security patches, and the provisioning of new services, and onboarding of new users. Building on this, a NaaS offering should include a foundational level of Incident detection, troubleshooting and remediation.

This all reduces the burden on in-house network staff, while removing the possibility that a forgotten or misconfigured manual update can create or amplify a security threat to a company.

The focus should be on the outcomes that the enterprise desires – consistent performance, support for remote locations, and optimization for unpredictable workloads – rather than what a traditional unchanging, underlying infrastructure permits.

## 4. What the advanced capabilities can – and should – be

> "Security policies can be everywhere in the network, providing a more consistent experience and policy for all devices regardless of location"

Adopting NaaS should provide a centralized, but far deeper view of the entire network, both within the bounds of the enterprise and beyond.

**Integrated and simplified security.** Each day, more and more applications, workloads, and devices are being added to the network, increasing the network's attack surface. This exponentially increases the amount of data and number of connections in a network, making it difficult to implement security properly. These issues are compounded by hackers using more sophisticated tools like artificial intelligence and machine learning to exploit networks.

But a NaaS solution with advanced security capabilities can improve an organization's security posture by merging network with security. NaaS can embed security into the network, blurring the lines between NetOps and SecOps and bringing the organizations together. Unifying network and security in NaaS, security policies can be everywhere in the network, providing a more consistent experience and policy for all devices regardless of location. SecOps obtains deeper insights into traffic flows and NetOps can incorporate network policy that works in tandem with security vs. against it. The end result is an easier-to-manage security policy with more insights than ever before.

**Network automation.** At the same time, NaaS delivers the potential for greater automation – quite how much can be decided between the supplier and the customer. But as a minimum, the onboarding of new users and new locations should move from being a manual chore to an automated, self-service process.

**Infrastructure as Code** (IaC) is the management and automated provisioning of network and infrastructure resources through code, instead of through manual processes. IaC products, like Terraform, can rapidly configure NaaS, LAN, fabric and other infrastructure resources and deploy applications on-premises and in public clouds. With IaC, configuration files are created that contain infrastructure specifications making it easier to edit and distribute configurations and optimize NaaS.

**DevOps and the application experience.** Going further, DevOps and related approaches to developing and deploying applications entail closer alignment between developer and infrastructure teams. Those continuous deployments mean continuous infrastructure interaction. One of the characteristics of the higher degrees of DevOps is self-service capability for managing infrastructure elements of the application. The policy centralization and automation that NaaS delivers, together with the flexibility and scalability it promises, are a natural fit with these modern development and deployment models.

Similarly, the focus on outcomes, as opposed to sometimes arbitrary SLAs focused on a narrow number of metrics, enables a closer focus on application experience wherever users or customers are.

**Deeper network insights.** The potentially far more integrated nature of NaaS should translate into improvements in telemetry capability across the domains where it is deployed. This provides a foundation for deeper insight into all NaaS-delivered parts of the network, automatically highlighting problems, and speeding their resolution. As trust grows, remediation should also increasingly become automated.

**Artificial intelligence.** AI is one of the factors shaping the modern technology landscape, and it is changing how enterprises and suppliers can exploit telemetry and insights, resulting in what can be termed AI Ops. This is represented by the shift from simple visibility to observability, whereby customers have the option to remediate an active issue or act once a potential issue has been highlighted or predicted. Increasingly, they can expect to hand this over to the network itself. This can apply to optimizing the network for workloads, or for particular types of users such as remote or home workers or spotting activity that could suggest a cyberattack or network breach.

Depending on the NaaS provider, this could extend to predicting when an application experience will degrade, an infrastructure component may be in danger of failure, or a certain public network service is overloaded, based on the provider's monitoring of other installations. This could then result in the pre-emptive offer of a scheduled replacement or maintenance visit. More advanced predictive maintenance could be offered for application experience degradations or Internet or cloud service degradations too. This could result in automated rerouting of traffic before any degradation is experienced. The extent of this lifecycle management will depend on the underlying vendor's own back-end capabilities and partnership network.

**APIs for integration.** A clear, open approach to APIs is central to NaaS, to underpin the integration of the

various security and management services. The reality is that many initial deployments of NaaS will be alongside existing infrastructure, and the two will co-exist for some time to come.

But a supplier's API approach is also central to allowing customers and partners to build the additional services they need on top of the network, and to integrate with the other tooling organizations rely on. For example, the existing IT system management systems and DevOps and Continuous Delivery tools developers will turn to for self-service deployment of infrastructure. When developers deploy the infrastructure, they use a service mesh that is logically split into a data plane and a control plane.

The data plane is composed of a set of intelligent proxies deployed as sidecars. These proxies mediate and control all network communication between microservices. They also collect and report telemetry on all mesh traffic. The control plane manages and configures the proxies to route traffic. All of this needs to be included in a NaaS and easy for developers to deploy.

## 5. NaaS - the operational perspective

> "Naturally, NetOps, CloudOps, SecOps, and AppOps should be part of the conversation"

**NaaS co-existing with traditional infrastructure.** As NaaS offerings become more widely available over the coming years, it is unlikely they will displace traditional networking approaches immediately.

There are situations where an organization decides on or is obliged to follow a more traditional approach. This could be dictated by specific regulatory or compliance requirements, depending on the industries or regions the organization operates in. And organizations will often have existing infrastructure that is nowhere near end-of-life or obsolete.

**Taking first steps.** As a first step, an organization considering NaaS might choose to consult with a NaaS provider or trusted partner to work out where NaaS fits with their current strategy and desired outcomes. They can also get a hands-on feel for NaaS through a limited pilot, perhaps by taking advantage of a try before you buy a program from a reputable vendor.

**Bringing together the right team.** All the relevant internal stakeholders should be part of the conversation. NaaS – affects the entire organization. Naturally, NetOps, CloudOps, SecOps, and AppOps should be part of the conversation.

Developer and DevOps teams should also contribute, given the extent to which NaaS can enable self-service infrastructure deployment. SRE teams on NaaS will ensure uptime and performance for the solution, but also Platform Engineering teams within customer domains will help define and influence the buying decisions on NaaS solutions.

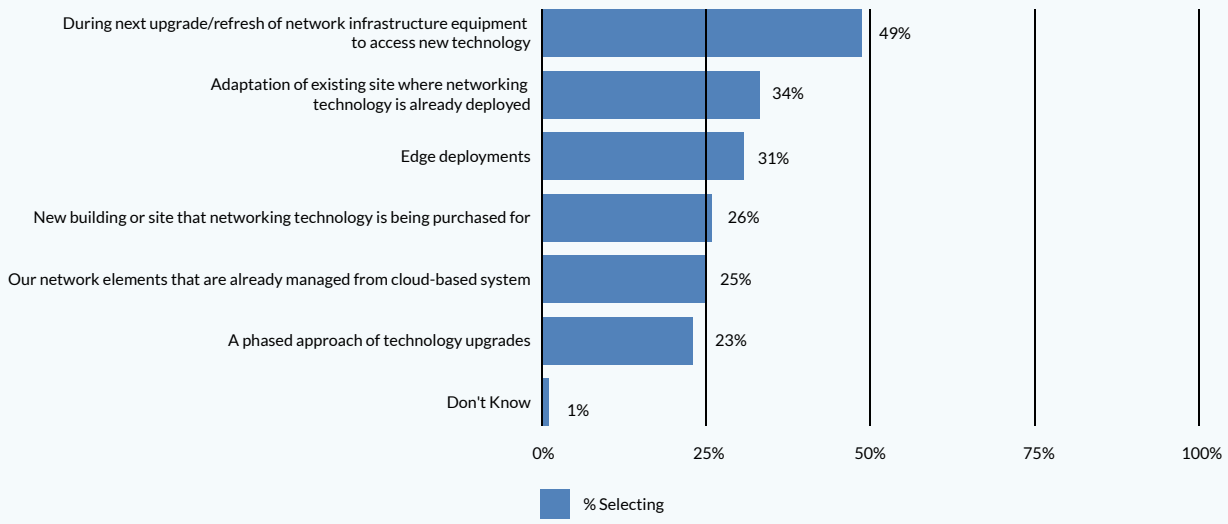
And given the implications for up-skill and role changes for existing and new staff, Human Resources should be part of the conversation. Also, a switch to NaaS changes budgeting considerations, as it entails a move from CapEx to OpEx spending. This means the Finance and procurement departments should also be involved from the outset.

**Where to start.** The essence of NaaS offers predictability, flexibility, and agility. Indeed, organizations may choose a phased approach to adopting NaaS. Recent IDC research showed half of respondents believed NaaS would be a best fit in their next network infrastructure refresh.

A good scenario might be to implement NaaS for a greenfield installation or service. For example, new branch offices could be serviced by NaaS from the start. For organizations where this is not applicable, the IT team could choose a specific low risk area or service in which to implement NaaS.

Alternatively, as organizations look to consolidate their data centers and other operational facilities, they could use this as an opportunity to implement NaaS.

**Q12. For which of the following scenarios do you believe NaaS would be the best fit for your organization? (n=1534)**




**Step-by-step.** Beyond that, an enterprise might choose a step-by-step approach, progressively moving more and more functionality to the NaaS provider. For example, just because an organization wants to adopt NaaS does not mean it must hand over complete control of security policies or threat management to a NaaS provider from the outset. Patching and updating could be handed off to the NaaS provider initially, while setting security policies and threat remediation could be reserved to in-house or trusted partner teams. Additional functions could then be delegated to the provider over time.

## 6. Implications for networking careers and skills

> "Over a quarter of IT leaders said the lack of necessary skills was a key obstacle to moving to an advanced network"

**Better utilizing talent.** Skilled networking and infrastructure talent are in perennial short supply. Before the pandemic, cloud, enterprise architecture and cybersecurity were amongst the top five "IT skills gaps" identified by IT and business executives, surveyed for Cisco's *2020 Global Networking Trends Report*.

Yet those highly skilled and sought-after technologists are then required to spend large parts of their working day maintaining and troubleshooting existing networks and their problems.

According to *2020 Global Networking Trends* respondents, maintenance takes up 55 percent of the typical networks team's time and resources. At the same time, over a quarter of IT leaders said the lack of necessary skills was a key obstacle to moving to an advanced network.

The same report cites "business acumen" as a key IT skills gap. Similarly, in 2019, AI and analytics, IT/IOT integration, and network DevOps are all seen as potential areas for improvement for networking teams.

Although other disciplines may have used the early lockdown days of COVID-19 to brush up on their skills, this was likely not an option for networking teams, as they bore the brunt of the burden of keeping organizations running as offices emptied.

**More time for value-adding tasks.** Some network professionals might be concerned that increased automation might reduce their role. However, adopting NaaS promises to reduce the amount of time spent dealing with repetitive, routine work, and remedying the problems spawned by complexity. This should free up time for professionals to address higher value work or strategic problems such as new digital engagement models for customers and employees, setting and

maintaining policies that best meet application and security needs, taking advantage of AI-enabled analytics to optimize the network, or to make more effective use of the possibilities of the cloud, including enabling the organization for hybrid and multi-cloud.

**Working across teams.** The transformational nature of NaaS – and the degree to which it integrates other functions – means that networking professionals should work closely with their counterparts in security, and other infrastructure disciplines. They will also work more closely with developers and line of business professionals, as they deliver on the self-service promise of NaaS.

Likewise, skilled staff will need to work closely with NaaS providers and partners, to establish the outcomes, experiences, financial objectives, and SLAs that the organization desires – and ensure that they are being met.

So, a NaaS rollout in no way means that the organization will be looking to reduce its networking team. Rather, it needs to plan to ensure that staff can make the transition to these higher value roles, ensuring the success of both the NaaS project, and the organization as a whole.

## 7. Why your NaaS vendor should work with partners

> "Partnerships and ecosystems will be essential to how organizations approach NaaS"

Choosing a NaaS vendor and/or partner should be a considered decision, whether the intention is to delegate as much of the network management as possible or to retain management of key functions.

Some enterprises might see simply adopting NaaS as an opportunity to bring all their networking, security and related operations under a single subscription, with a single supplier.

**Importance of partnerships and ecosystems.** But in reality, there is no one-size-fits-all NaaS. Organizations – like their networks – are complex. You need a service that fits into your operating model and can gradually integrate as your organization transitions to more as-a-Service consumption. So, partnerships and ecosystems will be essential to how organizations approach NaaS. The NaaS vendor's potential partners could include traditional channel industry specialists, managed service providers, or telcos and other communications providers.

**Thinking vertically.** Different verticals will have different needs. As stated above, a retailer's WAN endpoints (e.g. Point of Sales) needs may fluctuate season to season, and so the ability to scaleup connectivity while minimizing latency with payment providers is key. A financial services firm might have security uppermost in their mind, while also needing to comply with different data regulations in multiple countries. An energy firm might have a particular focus on managing and processing machine data, whether in the field or centrally.

So, the ability to partner with firms who have the scale and experience in delivering integrated, vertical specific solutions will be an important factor when choosing a NaaS vendor.

**Open and extensible.** Similarly, a vendor's approach to openness, and offering extensible APIs that you or your service integrator can take advantage of, should be considered.

**Location considerations.** And a NaaS vendor's regional coverage may be augmented by a strong partner network. Predictive analytics become moot when there is no capability to replace a component before it fails.

The partner or NaaS vendor should help the enterprise assess its current state of readiness for adopting NaaS and identify where it makes most sense to begin the transition. They should also help the customer evolve the SLAs or outcomes they want to work towards.

## 8. NaaS - financial considerations

**Beyond TCO and cost.** Organizations have been adopting flexible consumption of compute and storage infrastructure for several years. NaaS is part of this

broader trend. While for many organizations, financial benefits such as TCO and cost reduction are not the primary drivers for considering NaaS, the switch to cloud computing, flexible consumption, or x-as-a-service has several up-front financial advantages, which also apply to Network as a Service.

It removes the need to make a large upfront capital investment to upgrade or refresh networking infrastructure – and obviates the challenges and compromises that network specialists often face in securing budget and projects approved.

**Opex to Capex.** The switch to subscription-based pricing means that the network becomes an ongoing operating expense, rather than a periodic capital expense. Furthermore, depending on the precise nature of the contract, the ongoing cost is directly related to usage and consumption, potentially making spending much more predictable. Other possibilities include tying billing to SLAs, or the number of endpoints covered.

If circumstances demand a temporary increase in capacity, the associated costs for this should be transparent. If an organization wants to take advantage of new technology, the additional monthly cost – if any – should be clear, and predictable.

This means decisions about new technologies or services, or upgrades, can be made quickly, rather than triggering a complex out-of-lifecycle negotiation or being postponed to the next budget period.

None of this means that companies should not think seriously about the fiscal implications of NaaS from the outset. The switch from CapEx to OpEx may have broader budget implications. It makes sense for IT and financial teams to collaborate early on shaping the NaaS strategy.

**Other financial benefits.** There are other financial impacts beyond the straightforward costs of the NaaS subscription. Better integration and management of networking and security, as well as with the rest of the infrastructure, should lead to better resiliency, reducing downtime and associated costs for the entire business. Better optimization and utilization, and the knowledge that services can be easily scaled up, reduces the temptation to overprovision and so avoid the danger of stranded resources.

Conversely, enabling network ops staff to spend less time on routine maintenance and management frees them up to tackle more challenging work, ultimately leading to a better optimized, more agile network, and infrastructure in general. This in turn will better support the organization's digital transformation goals.

## Conclusion

> **"The network is no longer seen as an obstacle to continuous innovation, but the very thing that enables it"**

NaaS promises to revolutionize how organizations buy, implement, and manage networking in the future, all without the risk of a single "big bang" transition.

This solution reduces the total cost of connectivity and security for customers, and enables a switch to outcome driven experiences, underwritten by policy driven network management. Security becomes unified, end-to-end, and scalable, while unified-identity-based policies allow individuals to be more mobile without compromising on their network and cloud access. Costs become more predictable. And this can all be managed through a single pane of glass.

But the most exciting thing about NaaS is its potential to free networking teams from legacy technology AND management models. This means they can fully participate in positioning their organizations for the future, whether that is adopting new technologies, workloads and workflows, or dealing with new and unexpected challenges. This means the network is no longer seen as an obstacle to continuous innovation, but the very thing that enables it.

Explore Cisco+ as-a-service solutions and NaaS roadmap.

## About Cisco

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future. Discover more on The Network and follow us on Twitter.